RISK CONTROL METHOD AND DEVICE

TECHNICAL FIELD

[0001] The present application relates to the field of Internet information technology and computer technology, and in particular, to a risk control method and device.

BACKGROUND

[0002] With the development of Internet technology, more people use the Internet as a platform to perform various transactions, such as purchasing products and paying for electricity bills and phone bills. Apparently, people's life is more dependent on the Internet.

[0003] To provide more convenient services to people, software developers have developed a variety of application software, so that people can enjoy various convenient services provided by the Internet by using application software installed on smart terminal devices, personal computers, or other smart devices. In addition, developers constantly improve functions of the applications and simplify user operations, thereby making services more convenient.

[0004] For example, if user A needs to send a piece of sensitive information to (e.g., an account password, a payment behavior, etc.) to user B, two methods may be used in an actual operation:

[0005] Method 1: When sending the sensitive information to user B, user A inputs account information of user B, and sends the account information and the sensitive information to a server. The server identifies pre-stored information of user B (such as a name of user B) that corresponds to the account information, and pushes the identified information to user A. When it is determined that the pre-stored information is correct, user A triggers the server to send the sensitive information to user B.

[0006] Method 2: When sending the sensitive information to user B, user A inputs account information of user B, and sends the account information and the sensitive information to a server. The server can directly push the received sensitive

information to a user corresponding to the account information based on the received account information.

[0007] Apparently, operations in Method 2 are simpler than operations in Method 1. However, some study shows that Method 2 has a relatively high security risk. More specifically, when the user B's account information input by user A is actually user C's account information instead of user B's account information, and if user A has not identified any input error, loss can occur to user A once the server responds to the request of user A.

SUMMARY

[0008] In view of this, implementations of the present application provide a risk control method and device, to resolve the problem of low application software security caused by user mistakes in an existing technology.

[0009] The risk control method includes: receiving a payment request sent by a first user, and determining a user attribute of the first user, where the payment request includes identification information of a second user; searching a user attribute database for a user attribute of the second user corresponding to the identification information of the second user included in the payment request based on the identification information of the second user, where the user attribute database stores user attributes of different users; determining a user attribute similarity between the first user and the second user by using the user attribute of the first user and the user attribute of the second user, where the user attribute similarity is used to represent a possibility of establishing a social relationship between the first user and the second user; and performing, based on the user attribute similarity, risk control on the payment request sent by the first user.

[0010] The risk control device includes: a receiving unit, configured to receive a payment request sent by a first user, and determine a user attribute of the first user, where the payment request includes identification information of a second user; a search unit, configured to search a user attribute database for a user attribute of the second user corresponding to the identification information of the second user included in the payment request based on the identification information of the second user, where the user attribute database stores user attributes of different users; a determining unit, configured to determine a user attribute similarity between the first

user and the second user by using the user attribute of the first user and the user attribute of the second user, where the user attribute similarity is used to represent a possibility of establishing a social relationship between the first user and the second user; and a control unit, configured to perform, based on the user attribute similarity, risk control on the payment request sent by the first user.

[0011] The present application has the following beneficial effects:

[0012] In the implementations of the present application, the payment request sent by the first user is received, and the user attribute of the first user is determined, where the payment request includes the identification information of the second user; the user attribute database is searched for the user attribute of the second user corresponding to the identification information of the second user included in the payment request based on the identification information of the second user; the user attribute similarity between the first user and the second user is determined by using the user attribute of the first user and the user attribute of the second user; and risk control is performed, based on the user attribute similarity, on the payment request sent by the first user. In addition to responding to the payment request sent by the first user, a server needs to determine the user attribute similarity between the first user and the second user based on the user attribute of the second user included in the payment request and the user attribute of the first user, and determine whether the payment request sent by the first user is potentially incorrect based on the determined user attribute similarity. As such, low application software security caused by user mistakes can be effectively avoided, and payment security can be effectively improved.

BRIEF DESCRIPTION OF DRAWINGS

[0013] To describe the technical solutions in the implementations of the present application more clearly, the following briefly describes the accompanying drawings required for describing the implementations. Apparently, the accompanying drawings in the following description show merely some implementations of the present application, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0014] FIG. 1 is a flowchart illustrating a risk control method, according to an implementation of the present application;

[0015] FIG. 2 is a flowchart illustrating a risk control method, according to an implementation of the present application; and

[0016] FIG. 3 is a structural diagram illustrating a risk control device, according to an implementation of the present application.

DESCRIPTION OF EMBODIMENTS

[0017] In an actual application, to help payment operations between different users, a relatively simple operation method is provided. A source user can send a payment request to a server based on identification information of a target user. For example, user A needs to transfer 100 RMB to user B via an Internet platform. If user A completes the transfer via a third-party payment platform, user A can transfer 100 RMB to user B as long as user A provides a server of the third-party payment platform with identification information it registered on the third-party payment platform and the transfer amount. However, because the identification information registered by user B on the third-party payment platform may have a relatively low security level, the identification information may be similar to identification information of other users, for example, lI and ll. If the identification information of user B input by user A is incorrect, and user A is unaware of the error, fund loss can occur to user A, and fund transfer security may be compromised.

[0018] To achieve the purpose of the present application, the implementations of the present application provide a risk control method and device. In addition to responding to a payment request sent by a first user, a server needs to determine a user attribute similarity between the first user and a second user based on the second user's user attribute included in the payment request and the user attribute of the first user. The server then determines whether the payment request sent by the first user is potentially incorrect based on the determined user attribute similarity. As such, low application software security caused by user mistakes can be effectively reduced, and payment security can be effectively improved.

[0019] The risk control method provided in the implementations of the present application can be implemented based on a third-party payment platform, instant messaging software provided by a software developer, or other software having payment capabilities.

[0020] It is worthwhile to note that, a payment request described in the

implementations of the present application not only includes shopping payment (that is, a buyer purchases a product from a seller, and pays the seller accordingly), but can also include fund transfer between different users, and can even include sending virtual "red envelope" between different users. Specific implementations are not limited here.

[0021] User attributes described in the implementations of the present application can include location of the user when the user registers with the server, location of the user when the user sends a payment request, user's education background, user's job type, user's occupation, phone number used when the user registers with the server, and user's birthplace. Specific implementations are not limited in the present application.

[0022] A user attribute similarity described in the implementations of the present application can be the number of same user attribute types and contents shared between the user and third user. A larger number indicates a higher user attribute similarity, and a smaller number indicates a lower user attribute similarity.

[0023] Alternatively, a user attribute similarity can be a weight of a user attribute with the same attribute type and content shared between the user and third user. A larger weight indicates a higher user attribute similarity, and a smaller weight indicates a lower user attribute similarity.

[0024] "First" and "second" in "first user" and "second user" described in the implementations of the present application are merely used to distinguish between different users without indicating other special meanings.

[0025] The following further describes the implementations of the present application in detail with reference to the accompanying drawings in this specification. Apparently, the described implementations are merely some rather than all of the implementations of the present application. Other implementations obtained by a person of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0026] FIG. 1 is a flowchart illustrating a risk control method, according to an implementation of the present application. The method can be shown as follows:

[0027] Step 101: Receive a payment request sent by a first user, and determine a user attribute of the first user.

[0028] The payment request includes identification information of a second user.

[0029] In step 101, when the first user needs to make a payment to the second user, the first user sends the payment request to a server by using client software.

[0030] The client software here can be an APP having a payment capability developed by a third-party service platform, or can be an APP corresponding to a third-party payment platform. The client software is not limited here.

[0031] The server here is a server corresponding to the APP, that is, a server of the third-party service platform.

[0032] In step 101, the payment request sent by the first user includes the identification information of the second user. The identification information of the second user can be an email account, an instant messaging account, a phone number, a user name, a bank account, etc., which is not limited here.

[0033] When receiving the payment request sent by the first user, in an existing process, the server responds to the payment request when determining that an identity of the first user is valid. However, to improve user account security and fund security, the server needs to confirm the received payment request sent by the first user, that is, determine whether it is possible that the identification information of the second user is incorrectly input. How to determine whether the identification information of the second user may be incorrectly input is described below.

[0034] Before determining whether the identification information of the second user may be incorrectly input, the server needs to further determine the user attribute of the first user based on identification information of the first user or account information of the first user when the server receives the payment request from the first user.

[0035] More specifically, the server can determine the user attribute of the first user based on registration information of the first user and/or user behavior data of the first user, such as a registration address (e.g., Beijing) of the first user, an address (e.g., Shanghai) where the first user sends the payment request, the birthplace (e.g., Beijing) of the first user, and the place where the first user is often located (which can be determined based on historical behavior data of the user, etc.).

[0036] It is worthwhile to note that if the user attribute is address information, the address information of the user can be determined through GPS (the address information can include registration address, address of the user location, current address of a terminal device, etc). The address information of the user can be determined based on a wireless positioning service, or the address information of the

user can be determined by another positioning method, which is not limited here.

[0037] Determining a user attribute of the first user can include: searching a log information database for identification information of third user that has a social relationship with the identification information of the first user; and determining the user attribute of the first user if the identification information of the third user does not include the identification information of the second user.

[0038] When it is determined that the identification information of the third user includes the identification information of the second user, the identified identification information of the third user that is the same as the identification information of the second user is sent to the first user, and the first user is notified to confirm the identification information of the third user and the identification information of the second user.

[0039] In addition, when receiving the payment request sent by the first user, the server further needs to determine whether a payment has been previously performed between the first user and the second user. Because the user behavior data of the first user on an Internet platform is stored in the log information database of the server, it can be determined whether payment has occurred between the first user and the second user included in the payment request by searching the log information database. If it is identified from the log information database that the identification information of the third user that has a social relationship with the identification information of the first user does not include the identification information of the second user, it can indicate that payment between the first user and the second user occurred for the first time. Therefore, whether the identification information of the second user included in the payment request sent by the first user is incorrect needs to be estimated.

[0040] If it is identified from the log information database that the identification information of the third user that has a social relationship with the identification information of the first user includes the identification information of the second user, it indicates that the identification information of the third user that has made payment with the first user is the same as the identification information of the second user included in the payment request. If the identification information is an email address, a user name, an instant messaging identifier, etc that is not unique, the first user needs to be notified to determine whether the identification information of the second user is incorrect.

[0041] Specifically, the server can send the identified identification information of the third user that has the same identification information as the second user to the first user, and notifies the first user to confirm the identification information of the third user and the identification information of the second user.

[0042] Step 102: Search a user attribute database for a user attribute of a second user that corresponds to identification information of the second user included in the payment request based on the identification information of the second user.

[0043] The user attribute database stores user attributes of different users.

[0044] In step 102, the server determines the user attribute of the second user based on the identification information of the second user.

[0045] Here, the user attribute of the second user can be determined as follows: The user attribute database can be searched to identify the user attribute of the second user corresponding to the identification information of the second user, or the user attribute of the second user is determined based on registration information of the second user and/or user behavior data of the second user. The implementations of the method are not limited here.

[0046] The user attribute database described in this implementation of the present application can be a database for storing user attributes. Mapping relationships between identification information of users and user attributes can be established in the user attribute database, so that the user attributes can be determined by using the identification information of the user.

[0047] It is worthwhile to note that the identification information of the user can uniquely identify the user, and it can be a user ID, or multiple pieces of user identification information, such as a user name and an email address. Alternatively, a user ID that uniquely identifies each user can be generated for the user in the user attribute database. Other implementations are not limited here.

[0048] Step 103: Determine a user attribute similarity between the first user and the second user by using the user attribute of the first user and the user attribute of the second user.

[0049] The user attribute similarity is used to represent a possibility of establishing a social relationship between the first user and the second user.

[0050] In step 103, the number of user attributes with the same types and contents shared between the first user and the second user is calculated, and the user attribute similarity between the first user and the second user is determined based on the

number. A larger number corresponds to a higher user attribute similarity and a smaller number corresponds to a lower user attribute similarity.

[0051] Specifically, the types of the user attributes of the first user and the types of the user attributes of the second user are separately determined, user attributes with the same types shared between the first user and the second user are selected, and the number of user attributes with the same contents shared between the first user and the second user is determined from the user attributes of the same types.

[0052] The user attribute similarity between the first user and the second user is determined based on the number. A larger number corresponds to a higher user attribute similarity and a smaller number corresponds to a lower user attribute similarity.

[0053] In addition, a weight can also be determined for each user attribute type. To determine the user attribute similarity between the first user and the second user, a factor of a user attribute that is included in both the first user and the second user is set to 1. A factor of a user attribute exclusive to the first user or the second user is set to 0. A user attribute value of the first user and a user attribute value of the second user are separately calculated based on the weight and the factor and a difference between the user attribute value of the first user and the user attribute value of the second user is calculated. The obtained difference is the user attribute similarity between the first user and the second user.

[0054] It is worthwhile to note that the weight can be set based on impact of the user attribute on the possibility of establishing a social relationship between the first user and the second user. Stronger impact can result in a larger weight to be set, and a weaker impact can result in a smaller weight to be set. For example, impact of a family relationship is larger than impact of a friendly relationship.

[0055] Step 104: Perform, based on the user attribute similarity, risk control on the payment request sent by the first user.

[0056] In step 104, when the user attribute similarity is less than a specified threshold, a notification message is sent to the first user. The notification message is used to notify the first user to confirm the identification information of the second user included in the payment request; or when the user attribute similarity is not less than a specified threshold, a response is made to the payment request sent by the first user.

[0057] In the technical solution provided in this implementation of the present

application, the payment request sent by the first user is received and the user attribute of the first user is determined. The payment request includes the identification information of the second user. The user attribute database is searched to identify the user attribute of the second user that corresponds to the identification information of the second user included in the payment request based on the identification information of the second user. The user attribute database stores user attributes of different users. The user attribute similarity between the first user and the second user is determined by using the user attribute of the first user and the user attribute of the second user. The user attribute similarity is used to represent the possibility of establishing a social relationship between the first user and the second user. Risk control is performed, based on the user attribute similarity, on the payment request sent by the first user. In addition to responding to the payment request sent by the first user, the server needs to determine the user attribute similarity between the first user and the second user based on the user attribute of the second user included in the payment request and the user attribute of the first user. The server also determines whether the payment request sent by the first user may be incorrect based on the determined user attribute similarity. As such, low security caused by user mistakes can be effectively reduced, and payment security can be effectively improved.

[0058] FIG. 2 is a flowchart illustrating a risk control method, according to an implementation of the present application. The method can be described as follows:

[0059] Step 201: Receive a payment request sent by a first user.

[0060] The payment request includes identification information of a second user.

[0061] Step 202: Search a log information database for identification information of third user that has a social relationship with identification information of the first user.

[0062] Step 203: Determine whether the identified identification information of the third user includes identification information of a second user. If the identified identification information of the third user does not include the identification information of the second user, perform step 205. Otherwise, if the identified identification information of the third user includes the identification information of the second user, perform step 204.

[0063] Step 204: When it is determined that the identification information of the third user includes the identification information of the second user, send the identified identification information of the third user that is the same as the

identification information of the second user to the first user, and notify the first user to confirm the identification information of the third user and the identification information of the second user.

[0064] Step 205: Determine a user attribute of the first user when it is determined that the identification information of the third user does not include the identification information of the second user.

[0065] Step 206: Search a user attribute database for a user attribute of the second user corresponding to the identification information of the second user included in the payment request based on the identification information of the second user.

[0066] The user attribute database stores user attributes of different users.

[0067] Step 207: Determine a user attribute similarity between the first user and the second user by using the user attribute of the first user and the user attribute of the second user.

[0068] The user attribute similarity can be used to represent a possibility of establishing a social relationship between the first user and the second user.

[0069] Step 208: Perform, based on the user attribute similarity, risk control on the payment request sent by the first user.

[0070] In addition to responding to the payment request sent by the first user, a server needs to determine the user attribute similarity between the first user and the second user based on the user attribute of the second user included in the payment request and the user attribute of the first user, and determine whether the payment request sent by the first user may be incorrect based on the determined user attribute similarity. As such, low security caused by user mistakes can be effectively reduced, and payment security can be effectively improved.

[0071] FIG. 3 is a structural diagram illustrating a risk control device, according to an implementation of the present application. The risk control device includes a receiving unit 31, a search unit 32, a determining unit 33, and a control unit 34.

[0072] The receiving unit 31 is configured to receive a payment request sent by a first user and determine a user attribute of the first user. The payment request includes identification information of a second user.

[0073] The search unit 32 is configured to search a user attribute database for a user attribute of the second user corresponding to the identification information of the second user included in the payment request based on the identification information of the second user. The user attribute database stores user attributes of different users.

[0074] The determining unit 33 is configured to determine a user attribute similarity between the first user and the second user by using the user attribute of the first user and the user attribute of the second user. The user attribute similarity is used to represent a possibility of establishing a social relationship between the first user and the second user.

[0075] The control unit 34 is configured to perform, based on the user attribute similarity, risk control on the payment request sent by the first user.

[0076] In another implementation of the present application, that the receiving unit 31 determines the user attribute of the first user includes: searching a log information database for identification information of the third user that has a social relationship with identification information of the first user; and determining the user attribute of the first user when it is determined that the identification information of the third user does not include the identification information of the second user.

[0077] In another implementation of the present application, the risk control device further includes a sending unit 35.

[0078] The sending unit 35 is configured to: when it is determined that the identification information of the third user includes the identification information of the second user, send the identified identification information of the third user that is the same as the identification information of the second user to the first user, and notify the first user to confirm the identification information of the third user and the identification information of the second user.

[0079] In another implementation of the present application, that the determining unit 33 determines the user attribute similarity between the first user and the second user by using the user attribute of the first user and the user attribute of the second user includes: calculating the number of user attributes with the same types and contents shared between the first user and the second user, and determining the user attribute similarity between the first user and the second user based on the number. A larger number corresponds to a higher user attribute similarity and a smaller number corresponds to a lower user attribute similarity.

[0080] In another implementation of the present application, that the control unit 34 performs, based on the user attribute similarity, risk control on the payment request sent by the first user includes: when the user attribute similarity is less than a specified threshold, sending a notification message to the first user. The notification message is used to notify the first user to confirm the identification information of the

second user included in the payment request; or when the user attribute similarity is not less than a specified threshold, responding to the payment request sent by the first user.

[0081] It is worthwhile to note that the risk control device described in this implementation of the present application can be implemented by hardware, or can be implemented by software. Other implementations are not limited here.

[0082] In addition to responding to the payment request sent by the first user, the risk control device described in this implementation of the present application needs to determine the user attribute similarity between the first user and the second user based on the user attribute of the second user included in the payment request and the user attribute of the first user, and determine whether the payment request sent by the first user may be incorrect based on the determined user attribute similarity. As such, low security caused by user mistakes can be effectively reduced, and payment security can be effectively improved.

[0083] A person skilled in the art should understand that the implementations of the present application can be provided as a method, an apparatus (device), or a computer program product. Therefore, the present application can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. Moreover, the present application can use a form of a computer program product implemented on one or more computer-readable storage media (including but not limited to a magnetic disk memory, a CD-ROM, an optical memory, etc) that include computer readable program code.

[0084] The present application is described with reference to the flowcharts and/or block diagrams of the method, the apparatus (device), and the computer program product according to the implementations of the present application. It should be understood that computer program instructions can be used to implement each process and/or each block in the flowcharts and/or the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions can be provided for a general-purpose computer, a dedicated computer, an embedded processor, or a processor of another programmable data processing device to generate a machine, so that the instructions executed by the computer or the processor of the another programmable data processing device generate an apparatus for implementing a specified function in one

or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0085] These computer program instructions can be stored in a computer readable memory that can instruct the computer or the another programmable data processing device to work in a specific way, so that the instructions stored in the computer readable memory generate an artifact that includes an instruction apparatus. The instruction apparatus implements a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0086] These computer program instructions can be loaded to the computer or the another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or the another programmable device provide steps for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0087] Although some preferred implementations of the present application have been described, a person skilled in the art can make changes and modifications to these implementations once they learn the basic inventive concept. Therefore, the following claims are intended to be construed as to cover the preferred implementations and all changes and modifications falling within the scope of the present application.

[0088] Apparently, a person skilled in the art can make various modifications and variations towards the present application without departing from the spirit and scope of the present application. The present application is intended to cover these modifications and variations of the present application provided that they fall within the scope of protection described by the following claims and their equivalent technologies.

CLAIMS

1. A method for risk control, the method comprising:

receiving a payment request sent by a first user, wherein the payment request comprises identification information of a second user;

determining a user attribute of the first user (101);

searching a log information database for identification information of a third user that has a social relationship with identification information of the first user (202);

determining that the identification information of the third user comprises the identification information of the second user;

sending identification information of the third user that is the same as the identification information of the second user to the first user;

notifying the first user to confirm the identification information of the third user and the identification information of the second user;

searching a user attribute database for a user attribute of the second user corresponding to the identification information of the second user comprised in the payment request based on the identification information of the second user, wherein the user attribute database stores user attributes of different users (102);

determining a user attribute similarity between the first user and the second user by using the user attribute of the first user and the user attribute of the second user, wherein the user attribute similarity is used to represent a possibility of establishing a social relationship between the first user and the second user (103); and

performing, based on the user attribute similarity, risk control on the payment request sent by the first user (104).

2. The risk control method according to claim 1, wherein the user attribute of the first user comprises a first attribute content and an attribute type, wherein the user attribute of the second user comprises a second attribute content and the attribute type, and wherein determining the user attribute similarity comprises:

determining a weight value of the attribute type based on an impact of the attribute type on the possibility of establishing a social relationship between the first user and the second user; and

determining the user attribute similarity based on the weight value, the first attribute content, and the second attribute content.

3. The risk control method according to any one of claims 1 and 2, wherein determining the user attribute similarity between the first user and the second user comprises:

determining a plurality of user attributes of the first user and a plurality of user attributes of the second user;

calculating the number of user attributes with the same attribute types and attribute contents shared between the first user and the second user; and

determining the user attribute similarity between the first user and the second user based on the number, wherein a larger number corresponds to a higher user attribute similarity, and a smaller number corresponds to a lower user attribute similarity (207).

4. The risk control method according to claim 3, wherein performing, based on the user attribute similarity, risk control on the payment request sent by the first user comprises:

in response to determining that the user attribute similarity is less than a specified threshold, sending a notification message to the first user, wherein the notification message is used to notify the first user to confirm the identification information of the second user comprised in the payment request.

5. The risk control method according to claim 3, wherein the performing, based on the user attribute similarity, risk control on the payment request sent by the first user comprises:

in response to determining that the user attribute similarity is not less than a specified threshold, responding to the payment request sent by the first user.

6. A device for risk control, the device comprising a plurality of modules configured to perform the method according to any one of claims 1 to 5.